A Number Theoretic Approach to Sylow r-Subgroups of Classical Groups

Mashhour I. AlAli, Christoph Hering,

and Anni Neumann

Department of Mathematics
Mu'tah University
Alkarak — Jordan
masshour_ibrahim@yahoo.com

Mathematics Institute
University of Tübingen
Morgen Stelle 10
D-72076 Tübingen — Germany
hering@uni-tuebingen.de

Mathematics Institute
University of Tübingen
Morgen Stelle 10
D-72076 Tübingen — Germany
drvneuman@web.de

Recibido: 20 de Enero de 2003
Aceptado: 28 de Enero de 2005

ABSTRACT

The purpose of this paper is to give a general and a simple approach to describe the Sylow r-subgroups of classical groups.

Key words: Sylow r-subgroups, wreath product.

2000 Mathematics Subject Classification: 20D15.

Introduction

Let G be a finite classical group over a finite field of characteristic p. The Sylow r-subgroups of G, where r is a prime number, have been given by Weir [5] in the case $r \neq 2$, $r \neq p$, and by Chevalley [3] and Ree [4] in the case $r = p$. In the later case the normalizers of the Sylow p-subgroups were obtained as well. The remaining case $r = 2$, $p \neq 2$ has been investigated by Carter and Fong [2], where the description is not easy to follow.

ISSN: 1139-1138
http://dx.doi.org/10.5209/rev_REMA.2005.v18.n2.16676

The main purpose of this paper is to give a more general and simple approach to describe the Sylow r-subgroups of the general linear group $\mathrm{GL}(n, q)$, the symplectic group $\mathrm{Sp}(2n, q)$ over $\mathrm{GF}(q)$, $q = p^a$, and the symmetric group S_n, using number theoretic techniques, so that general readers simply can read it. Among other results the conditions on r and G forcing the Sylow r-subgroups of $\mathrm{GL}(n, q)$ to be maximal nilpotent are given.

Let V be a n-dimensional vector space over $\mathrm{GF}(q)$. In the case of $\mathrm{GL}(V) = \mathrm{GL}(n, q)$, if d is a divisor of n, we consider the set $\{ V_1, V_2, \dots, V_m \}$ of d-dimensional subspaces such that $V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$, where $m = n/d$. Then the stabilizer of this set in $\mathrm{GL}(V)$ is obviously a wreath-product $\mathrm{GL}(V_1) \wr S_m$. Then we show that for any prime $r \neq p$, the number d can be chosen in such a way that this stabilizer contains a Sylow r-subgroup. Hence the Sylow r-subgroups are of the form $R \wr T_m \leq \mathrm{GL}(V_1) \wr S_M$, where R is a Sylow r-subgroup of $\mathrm{GL}(V_1)$ and T_m is a Sylow r-subgroup of S_m. From this description the action of the Sylow r-subgroups on the underlying vector space are obvious.

The approach for the other classical groups is quite similar. Let V be a vector space endowed with a bilinear, unitary or quadratic form. Then we consider an orthogonal decomposition $V = V_1 \perp V_2 \perp \cdots \perp V_m$ into non-degenerate subspaces of equal dimension d say. The stabilizer of the set $\{ V_1, V_2, \dots, V_m \}$ is then obviously isomorphic to $I(V_1) \wr S_m$, where $I(V_1)$ denotes the isometry group of V_1. Again by choosing d properly we find the Sylow r-subgroups are contained in such stabilizer and hence are isomorphic to $R \wr T_m$ where R is a Sylow r-subgroup of $I(V_1)$ and T_m is a Sylow r-subgroup of S_m. Also the action on the underlying vector space can be immediately seen.

1. Notation and basic definitions

Let n be an integer, p prime, we denote by n_p the p part of n. If G is a finite group, then $|G|$ denotes the order of G. If p is prime $\mathbb{Z}_{p-1}$ will denote the multiplicative cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ of the finite field $\mathrm{GF}(p)$. If $g \in G$, $o(g)$ denotes the order of g. Throughout the paper r, p are primes, $r \neq p$, and $q = p^a$. $H \wr K$ denotes the wreath product of H by K. For more information about the wreath product see [1]. $[H : K]$ denotes the index of K in H. We write X^m for a direct product of m copies of X.

2. The Sylow r-subgroups of $\mathrm{GL}(n, q)$

To investigate the Sylow r-subgroups of $\mathrm{GL}(n, q)$, we prove the following Lemmata which are of fundamental importance in this investigation.

Lemma 2.1. *Let d be the order of $q + r\mathbb{Z} \in (\mathbb{Z}/r\mathbb{Z})^*$, then $(q^i - 1)_r \neq 1$ if and only if $d \mid i$.*

Proof. Since $|\mathrm{GL}(n,q)| = q^{\binom{n}{2}} \prod_{i=1}^{n}(q^i - 1)$, we have $|\mathrm{GL}(n,q)|_r = \prod_{i=1}^{n}(q^i - 1)_r$. It is clear that $r \mid q^i - 1$ if and only if $(q + r\mathbb{Z})^i = 1 + r\mathbb{Z}$, and $(q + r\mathbb{Z})^i = 1 + r\mathbb{Z}$ iff $d \mid i$. Hence the Lemma is proved. □

Lemma 2.2. *If $r \mid q - 1$, then the following properties hold:*

(i) *If $r \neq 2$, then $(q^i - 1)_r = i_r(q - 1)_r$.*

(ii) *If $r = 2$ and $q \equiv 1 \pmod 4$, then $(q^i - 1)_2 = i_2(q - 1)_2$.*

(iii) *If $r = 2$, and $q \equiv 3 \pmod 4$, then*

$$(q^i - 1)_2 = \begin{cases} 2, & \text{if } i \text{ is odd,} \\ i_2(q+1)_2 & \text{if } i \text{ is even.} \end{cases}$$

Proof. Since $r \mid q - 1$ we write $q = 1 + r^a x$ for $a \geq 1$ and $\gcd(r, x) = 1$. On the other hand, $q^i - 1 = (q-1)(1+q+\cdots+q^{i-1})$ implies $(q^i - 1)_r = (q-1)_r(1+q+\cdots+q^{i-1})_r$. Since $q \equiv 1 \pmod r$ then $1 + q + \cdots + q^{i-1} \equiv i \pmod r$.

(i) Case 1: $r \nmid i$. Then $(1 + q + \cdots + q^{i-1})_r = 1$ and we are done.

Case 2: $r|i$. So $i = r^b j$ with $\gcd(j, r) = 1$. We need to prove that $(1 + q + \cdots + q^{i-1})_r = r^b$.

Since $q^i - 1 = q^{r^b j} - 1 = (q^j - 1)(q^{j(r^b-1)} + \cdots + q^{2j} + q^j + 1)$ then $(q^i - 1)_r = (q^j - 1)_r(q^{j(r^b-1)} + \cdots + q^j + 1)_r = (q - 1)_r(q^{j(r^b-1)} + \cdots + q^j + 1)_r$, by case 1. We have also $q^{j(r^b-k)} = (1 + r^a x)^{j(r^b-k)} \equiv 1 + j(r^b - k)r^q x \pmod{r^{2a}}$. Thus,

$$1 + \sum_{k=1}^{r^b-1} q^{j(r^b-k)} \equiv r^b\Big(1 + jr^a x(r^b - 1) - jr^a x\frac{r^b - 1}{2}\Big) \pmod{r^{2a}}$$

because $r \neq 2$. Therefore

$$(1 + q^j + \cdots + q^{j(r^b-1)})_r = r^b.$$

(ii) We consider the following two cases:

Case 1: i is odd. Then $1 + q + \cdots + q^{i-1}$ is odd, and this implies $(q^i - 1)_2 = (q - 1)_2(1 + q + \cdots + q^{i-1})_2 = (q - 1)_2 = i_2(q - 1)_2$.

Case 2: i is even. So $i = 2j$ and $(q^i - 1)_2 = (q^{2j} - 1)_2 = (q^j - 1)_2(q^j + 1)_2$. Since $q \equiv 1 \pmod 4$ this implies $q^j + 1 \equiv 2 \pmod 4$. Hence $(q^i - 1)_2 = (q^j - 1)_2 \cdot 2 = j_2(q - 1)_2 \cdot 2 = i_2(q - 1)_2$ by induction.

(iii) Again we have two cases:

Case 1: i is odd. Then $(q^i-1)_2 = (q-1)_2(1+q+\cdots+q^{i-1})_2 = (q-1)_2 = 2$.

Case 2: i is even. So $i=2j$ and since $q^2 \equiv 1 \pmod 4$, then by (ii) we have $(q^i-1)_2 = (q^{2j}-1)_2 = j_2(q^2-1)_2 = j_2(q-1)_2(q+1)_2 = j_2 \cdot 2 \cdot (q+1)_2 = i_2(q+1)_2$. □

Lemma 2.3. *Let r and p be distinct primes, $q=p^a$, and $d=o(q+r\mathbb{Z})$ where $q+r\mathbb{Z} \in (\mathbb{Z}/r\mathbb{Z})^*$ then the following properties hold:*

(i) *If either $r \neq 2$ or $r=2$ and $q \equiv 1 \pmod 4$, then $|\operatorname{GL}(n,q)|_r = (q^d-1)_r^{[\frac{n}{r}]}([\frac{n}{d}]!)_r$.*

(ii) *If $r=2$, $q \equiv 3 \pmod 4$ and n is even, then $|\operatorname{GL}(n,q)|_r = (2^2(q+1)_2)^{\frac{n}{2}}((n/2)!)_2$.*

(iii) *If $r=2$, $q\equiv 3 \pmod 4$ and n is odd, then*

$$|\operatorname{GL}(n,q)|_r = 2\Bigg(2^{n-1} \prod_{\substack{i\le n\\ i\ even}} i_2(q+1)_2\Bigg).$$

Proof. (i) We have

$$|\operatorname{GL}(n,q)|_r = \left| q^{\binom{n}{2}} \prod_{i=1}^{n}(q^i-1)\right|_r = \prod_{i=1}^{n}(q^i-1)_r = \prod_{i\le n,\ d|i}(q^i-1)_r.$$

By Lemma 2.1, $r \mid q^i-1$ iff $d \mid i$. We obtain $\prod_{i\le n,\ d|i}(q^i-1)_r = \prod_{j=1}^{[\frac{n}{d}]}(q^{dj}-1)_r$ and by Lemma 2.2, with q replaced by q^d, we obtain

$$\prod_{j=1}^{[\frac{n}{d}]}(q^{dj}-1)_r = \prod_{j=1}^{[\frac{n}{d}]} j_r(q^d-1)_r = (q^d-1)_r^{[\frac{n}{d}]}\prod_{j=1}^{[\frac{n}{d}]} j_r = (q^d-1)_r^{[\frac{n}{d}]}\Big(\Big[\frac{n}{d}\Big]!\Big)_r.$$

Hence a Sylow r-subgroup of $\operatorname{GL}(n,q)$ is isomorphic to $Z_{(q^d-1)_r} \wr T_{[\frac{n}{d}]}$, where $T_{[\frac{n}{d}]}$ is a Sylow r-subgroup of $S_{[\frac{n}{d}]}$.

(ii) $|\operatorname{GL}(n,q)|_2 = \prod_{i=1}^{n}(q^i-1)_2$. Let $n=2n_1$ for some integer n_1, then we have

$$\begin{aligned}\prod_{i=1}^{n}(q^i-1)_2 &= \prod_{j=0}^{n-1}(q^{2j+1}-1)_2\prod_{j=1}^{n_1}(q^{2j}-1)_2 = \\ &= 2^{n/2}\prod_{j=1}^{n/2}(q^{2j}-1)_2 = 2^{n/2}\prod_{j=1}^{n/2}(2j)_2(q+1)_2 = \\ &= 2^n(q+1)_2^{n/2}\prod_{j=1}^{n/2} j_2 = 2^n(q+1)_2^{n/2}(n/2)! = (2^2(q+1)_2)^{n/2}((n/2)!)_2.\end{aligned}$$

Hence if n is even and $q \equiv 3 \pmod 4$, then a Sylow 2-subgroup of $\mathrm{GL}(n,q)$ is isomorphic to $D \wr T$ where D is a Sylow 2-subgroup of $\mathrm{GL}(2,q)$ and T is a Sylow 2-subgroup of the symmetric group $S_{n/2}$.

(iii) We have

$$\begin{aligned}|\mathrm{GL}(n,q)|_2 &= \prod_{i=1}^{n}(q^i-1)_2 = \prod_{\substack{i\le n\\ i \text{ odd}}} 2 \prod_{\substack{i\le n\\ i \text{ even}}} (q^i-1) = \\ &= 2^n \prod_{\substack{i\le n\\ i \text{ even}}} i_2(q+1)_2 = 2\cdot 2^{n-1} \prod_{\substack{i\le n\\ i \text{ even}}} i_2(q+1)_2.\end{aligned}$$

Hence, if n is odd and $q \equiv 3 \pmod 4$, then a Sylow 2-subgroup of $\mathrm{GL}(n,q)$ is isomorphic to $Z_2 \times S \le \mathrm{GL}(1,q) \times \mathrm{GL}(n-1,q) \le \mathrm{GL}(n,q)$, where S is a Sylow 2-subgroup of $\mathrm{GL}(n-1,q)$. The Sylow r-subgroups of S_n will be discussed in section 4. □

Combining Lemma 2.1 and Lemma 2.2 we have

Lemma 2.4. *Let r and p be distinct primes, $q = p^a$. Define $d = o(q + r\mathbb{Z})$ where $q + r\mathbb{Z} \in (\mathbb{Z}/r\mathbb{Z})^*$, then we have*

(i) *$r \mid q^i - 1$ iff $d \mid i$.*

(ii) *If $d \mid i$ and either $r \ne 2$, or $r = 2$ and $q \equiv 1 \pmod 4$, then $(q^i-1)_r = (\frac{i}{d})_r(q^d-1)_r$.*

(iii) *If $d \mid i$, $r = 2$, and $q \equiv 3 \pmod 4$, then*

$$(q^i-1)_r = \begin{cases} 2, & \text{if } i \text{ is odd,}\\ i_2(q+1)_2, & \text{if } i \text{ is even.}\end{cases}$$

Remark 2.5. For $\mathrm{GL}(n,q)$ there are obviously subgroups of the orders calculated above. $\mathrm{GL}(n,q)$ contains the group of the monomial matrices $M \cong Z_{q-1} \wr S_n$. So in the case $r \mid q-1$, M contains a Sylow r-subgroup. In general, set $d = o(q + r\mathbb{Z})$ and write $n = n_0 d + n_1$ for integers n_0, n_1 with $0 \le n_1 < d$, then we have a canonical embedding of $\mathrm{GL}(n_0 d, q)$ into $\mathrm{GL}(n,q)$ as follows. Let V be a vector space of dimension n over $\mathrm{GF}(q)$ and write $V = V_0 \oplus V_1$ where $\dim V_0 = n_0 d$, $\dim V_1 = n_1$, so, if $H = \mathrm{GL}(V_1) \times \mathrm{GL}(V_0)$, then $C_H(V_0) \cong \mathrm{GL}(V_1) = \mathrm{GL}(n_1,q)$ and $C_H(V) \cong \mathrm{GL}(V_0) = \mathrm{GL}(n_0 d, q)$. Further, if W is a vector space of dimension n_0 over $\mathrm{GF}(q^d)$, then W is also a vector space over a subfield $\mathrm{GF}(q) \subseteq \mathrm{GF}(q^d)$ of dimension $n_0 d$, hence we have a canonical embedding $\mathrm{GL}(W) \subseteq \mathrm{GL}(V)$ or $\mathrm{GL}(n_0, q^d) \subseteq \mathrm{GL}(n_0 d, q)$. So we get a sequence of embeddings $\mathrm{GL}(n_0,q^d) \subseteq \mathrm{GL}(n_0 d, q) \subseteq \mathrm{GL}(n_0 d + n_1, q) = \mathrm{GL}(n,q)$, and $\mathrm{GL}(n_0,q^d)$ contains a monomial group $M^* \cong Z_{q^d-1} \wr S_{n_0}$ which contains, as we have shown above, a Sylow r-subgroup.

3. The Sylow r-subgroups of $\mathrm{Sp}(2n, q)$

To describe the Sylow r-subgroups of $\mathrm{Sp}(2n, q)$ we prove the following Lemmas.

Lemma 3.1. *Let r and p be distinct primes, $q = p^a$ and r odd, then*

(i) $\mathrm{Sp}(2n, q)$ *contains canonically a subgroup H isomorphic to* $\mathrm{GL}(n, q)$*.*

(ii) *If d is odd, then r does not divide the index of H in* $\mathrm{Sp}(2n, q)$*, where $d = o(q+\mathbb{Z})$, $q + \mathbb{Z} \in (\mathbb{Z}/r\mathbb{Z})^*$.*

(iii) *Any canonically embedded* $\mathrm{GL}(n, q)$ *contains a Sylow r-subgroup of* $\mathrm{Sp}(2n, q)$*.*

Proof. (i) Consider a symplectic base with respect to which the inner product matrix is $\left[\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right]$. Then the subgroup

$$H = \left\{ \begin{bmatrix} g & \\ & (g^t)^{-1} \end{bmatrix}, \quad g \in \mathrm{GL}(n, q) \right\}$$

is contained in the corresponding symplectic group $\mathrm{Sp}(2n, q)$.

The index of H in $\mathrm{Sp}(2n, q)$ is

$$\frac{q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)}{q^{\binom{n}{2}} \prod_{i=1}^{n} (q^i - 1)} = q^{n(n+1)/2} \prod_{i=1}^{n} (q^i + 1).$$

(ii) Assume that $r \mid q^{n(n+1)/2} \prod_{i=1}^{n}(q^i + 1)$. This implies that $r \mid q^i + 1$ for some $1 \leq i \leq n$, so $r \mid q^{2i} - 1$. This means that $q^{2i} \equiv 1 \pmod r$, thus $d \mid 2i$. As d is odd, this implies that $q^i \equiv 1 \pmod r$. Hence $r \mid q^i + 1$ and $r \mid q^i - 1$, thus $r \mid 2$, a contradiction.

(iii) As $r \nmid [\mathrm{Sp}(2n, q) : H]$, then H contains a Sylow r-subgroup and the Sylow r-subgroups of $\mathrm{GL}(n, q)$ have been determined in section 2. $\square$

Remark 3.2. If $n = n_1 + n_2$, then $\mathrm{Sp}(2n, q)$ contains a canonically embedded subgroup $\mathrm{Sp}(2n_1, q) \times \mathrm{Sp}(2n_2, q)$. This can be seen as follows. If V_1 and V_2 are symplectic spaces, then $V_1 \oplus V_2$ can be turned into a symplectic space, such that V_1 and V_2 are orthogonal. Let β_i be a symplectic form on V_i, $i = 1, 2$. Define a symplectic form β on $V_1 \oplus V_2$ by $\beta(v_1 + v_2, v_1' + v_2') = \beta_1(v_1, v_1') + \beta_2(v_2, v_2')$ where $v_i, v_i' \in V_i$. At the same time, this defines an embedding of $\mathrm{Sp}(V_1) \times \mathrm{Sp}(V_2)$ into $\mathrm{Sp}(V_1 \perp V_2)$. Here $V_1 \perp V_2$ denotes that V_1 and V_2 are orthogonal by the action

$$(v_1, v_2)^{(g_1, g_2)} = (v_1^{g_1}, v_2^{g_2})$$

where $v_1 \in V_1$, $v_2 \in V_2$, and $g \in \mathrm{Sp}(V_1)$, $g_2 \in \mathrm{Sp}(V_2)$. So we have a canonical embedding $\mathrm{Sp}(2n_1, q) \times \mathrm{Sp}(2n_2, q) \subseteq \mathrm{Sp}(2(n_1 + n_2), q)$. Repeating this process we get an embedding

$$\mathrm{Sp}(2n_1, q) \times \mathrm{Sp}(2n_2, q) \times \cdots \times \mathrm{Sp}(2n_k, q) \subseteq \mathrm{Sp}(2(n_1 + n_2 + \cdots + n_k), q),$$

for any $n_i \neq 0$. We have also an embedding $\mathrm{Sp}(2n, q)^k \subseteq \mathrm{Sp}(2nk, q)$.

The following Lemma is an immediate consequence of the above remark.

Lemma 3.3. *Let W be a symplectic space, and assume that W can be written as an orthogonal direct sum of $V_1 \perp V_2 \perp \cdots \perp V_k$ of subspaces V_i all of the same dimension. Let H be the stabilizer of $\{V_1, V_2, \ldots, V_k\}$ in $\mathrm{Sp}(W)$, then $H \cong \mathrm{Sp}(V_1) \wr S_k$.*

Lemma 3.4. *Let r and p be distinct primes, $q = p^a$. Let $d = o(q + r\mathbb{Z})$ where $q + r\mathbb{Z} \in Z_{r-1}$. If d is even, then*

$$|\mathrm{Sp}(2n, q)|_r = (q^d - 1)_r^{[\frac{2n}{d}]} \Big(\Big[\frac{2n}{d}\Big]!\Big)_r.$$

Proof. Let $d = 2t$ for some integer t. Then

$$|\mathrm{Sp}(2n, q)|_r = \prod_{i=1}^{n} (q^{2i} - 1)_r = \prod_{\substack{i=1\\ d|2i}}^{n} (q^2 i - 1)_r = \prod_{\substack{i=1\\ t|i}}^{n} (q^{2i} - 1)_r$$

By setting $i = tj$ we have

$$\prod_{\substack{i=1\\ t|i}}^{n} (q^{2i-1})_r \;=\; \prod_{j=1}^{[\frac{n}{t}]} (q^{dj} - 1)_r.$$

By Lemma 2.4, we obtain

$$\prod_{j=1}^{[\frac{n}{t}]} j_r (q^d - 1)_r = (q^d - 1)_r^{[\frac{n}{t}]} \prod_{j=1}^{[\frac{n}{t}]} j_r = (q^d - 1)_r^{[\frac{n}{t}]} \Big(\Big[\frac{n}{t}\Big]!\Big)_r =$$

$$= (q^d - 1)_r^{[\frac{2n}{d}]} \Big(\Big[\frac{2n}{d}\Big]!\Big)_r. \qquad \square$$

Theorem 3.5. *Let r be an odd prime, $r \neq p$, $q = p^a$, and $d = o(q + r\mathbb{Z})$. Then the following hold:*

(i) *If d is odd, then any canonically embedded $\mathrm{GL}(n, q)$ contains a Sylow r-subgroup of $\mathrm{Sp}(2n, q)$.*

(ii) *If d is even, $d = 2t$ for $1 \leq t \leq n$ and $n = at + b$ for $0 \leq b < t$, then any canonically embedded subgroup $\mathrm{Sp}(2t, q) \wr S_a \times \mathrm{Sp}(2b, q)$ contains a Sylow r-subgroup of $\mathrm{Sp}(2n, q)$ which is isomorphic to $Z_{(q^t-1)_r} \wr T$, where T is a Sylow r-subgroup of S_a.*

Proof. (i) It follows from Lemma 3.1.

(ii) It is an immediate consequence of Lemma 3.3 and Remark 2.5. $\square$

Revista Matemática Complutense
2005, 18; Núm. 2, 329–338

We are left with the remaining case $r = 2$, which will be settled by the following theorem.

Theorem 3.6. *The Sylow* 2*-subgroups of* $\mathrm{Sp}(2n, q)$ *are* $D \wr T$ *where* D *is a Sylow* 2*-subgroup of* $\mathrm{Sp}(2, q) = \mathrm{SL}(2, q)$*,* T *is a Sylow* 2*-subgroup of* S_n*, and* q *is odd.*

Proof. By Lemma 2.4, we obtain

$$|\mathrm{Sp}(2n, q)|_2 = \prod_{i=1}^{n} (q^{2i} - 1)_2 = \prod_{i=1}^{n} i_2(q^2 - 1)_2 = (q^2 - 1)_2^n (n!)_2.$$

So we have an orthogonal decomposition subgroup $\mathrm{Sp}(2, q) \wr Sn \leq \mathrm{Sp}(2n, q)$. Hence the Sylow 2-subgroups of $\mathrm{Sp}(2n, q)$ are as in the Theorem. □

4. The Sylow r-subgroups of the symmetric group S_n

To complete the description of the Sylow r-subgroups of $\mathrm{GL}(n, q)$ and $\mathrm{Sp}(2n, q)$, we investigate the Sylow r-subgroups of S_n. The following results are useful.

Lemma 4.1. *Let* r *and* p *be different primes. If* $n = pm + r$*,* $0 \leq r < p$*. Then* $(n!)_p = p^m([\frac{n}{p}]!)_p$*.*

Proof. We have the identities

$$(n!)_p = \prod_{i=1}^{n} i_p = \prod_{j=1}^{[\frac{n}{p}]} (jp)_p = \prod_{j=1}^{[\frac{n}{p}]} pj_p = p^{[\frac{n}{p}]} \prod_{j=1}^{[\frac{n}{p}]} j_p = p^{[\frac{n}{p}]} \big([\tfrac{n}{p}]!\big)_p. \qquad \square$$

Corollary 4.2. *A Sylow* p*-subgroup of* S_n *is isomorphic to* $Z_p \wr T$*, where* Z_p *is a Sylow* p*-subgroup of* S_p *and* T *is a Sylow* p*-subgroup of* S_m*.*

Theorem 4.3. *If* T_n *is a Sylow* p*-subgroup of* S_n*, then* $T_n = Z_p \wr (Z_p \wr (Z_p \wr T_{[n/p^3]}))$*. (It is a recursive relation.)*

Proof. Let S_n act on a set Ω of size n. Let $n = pm + r$, where $0 \leq r < p$. Consider a partition of Ω by the sets A_1, A_2,..., A_m, Γ, where $|A_i| = p$ and $|\Gamma| = r$. We have that $\Omega = \bigcup_{i=1}^{m} A_i \cup \Gamma$ is a disjoint union. The stabilizer of this partition in S_n is $H = (S_p \wr S_m) \times S_r$, which contains a subgroup $S = Z_p \wr T$ where Z_p is a Sylow p-subgroup of S_p and T is a Sylow p-subgroup of S_m. By changing the orders we see that if T_n is a Sylow p-subgroup of S_n, then $T_n = Z_p \wr T_{[n/p]}$ where $T_{[n/p]}$ is a Sylow p-subgroup of $S_{[n/p]}$, and $T_{[n/p]} = Z_p \wr T_{[[n/p]/p]} = Z_p \wr T_{[n/p^2]}$. Hence $T_n = Z_p \wr (Z_p \wr T_{[n/p^2]}) = Z_p \wr (Z_p \wr (Z_p \wr T_{[n/p^3]}))$. It is a recursive relation. □

5. A question

What are the conditions on r and q that force the Sylow r-subgroups of $\mathrm{GL}(n,q)$ to be maximal nilpotent? To answer this question we prove the following theorem.

Theorem 5.1. *Let r, p be two distinct primes, $d = o(q+r\mathbb{Z})$ where $q+r\mathbb{Z} \in (\mathbb{Z}/r\mathbb{Z})^*$. Suppose that $n = md+k$, $0 \le k < d$, and R is a Sylow r-subgroup of $\mathrm{GL}(n,q)$. If R is maximal nilpotent, then $n \equiv 0, 1 \pmod d$ and $q^d - 1 = r^i$ for some positive integer i.*

Proof. Let S be a Sylow r-subgroup of $\mathrm{GL}(d,q)$. By Schur's Lemma S is cyclic and $|S| = (q^d-1)_r$. If R is a Sylow r-subgroup of $\mathrm{GL}(n,q)$, then $R = S \wr T$ where T is a Sylow r-subgroup of S_m.

In a matrix form,

$$S = \left\{ \begin{bmatrix} x_1 & & & & \\ & x_2 & & & \\ & & \ddots & & \\ & & & x_m & \\ & & & & I \end{bmatrix} \middle| \; x_i \in S \right\},$$

where x_i is a $d \times d$ matrix and I is the identity $k \times k$ matrix. Now we prove that $C_{\mathrm{GL}(n,q)}(R)$ is contained in R if R is maximal nilpotent.

Let $x \in C_{\mathrm{GL}(n,q)}(R)$. This implies that $\langle R, x\rangle$ is again nilpotent. Since R is maximal nilpotent, it follows that $R = \langle R, x\rangle$. Thus $x \in R$. It is obvious that all elements

$$\begin{bmatrix} x & & & & \\ & x & & & \\ & & \ddots & & \\ & & & x & \\ & & & & K \end{bmatrix},$$

where K is any $k \times k$ matrix and $x \in C_{\mathrm{GL}(d,k)}(S)$, are contained in $C_{\mathrm{GL}(n,q)}(R)$. So if R is maximal nilpotent, all these elements must be contained in R. Finally, set

$$U = \left\{ \begin{bmatrix} x & & & & \\ & x & & & \\ & & \ddots & & \\ & & & x & \\ & & & & K \end{bmatrix} \middle| \; x \in C_{\mathrm{GL}(d,q)}(S), \quad K \in \mathrm{GL}(k,q) \right\}.$$

Then $U \le C_{GL(n,q)}(R)$. So, if R is maximal nilpotent, this implies $U \le R$ and hence U must be a r-group. Thus $|U| = |C_{\mathrm{GL}(d,q)}(S)|\,|\mathrm{GL}(k,q)| = (q^d-1)|\mathrm{GL}(k,q)|$ must be a power of r. Thus $d^q - 1 = r^i$ and $|\mathrm{GL}(k,q)| = r^j$, this implies, k must be at most 1, hence $k = 0$ or 1, which means $n \equiv 0, 1 \pmod d$. □

Acknowledgements. The authors are grateful to Hans J. Schaeffer for his helpful discussions.

References

[1] M. Aschbacher, *Finite group theory*, Cambridge Studies in Advanced Mathematics, vol. 10, Cambridge University Press, Cambridge, 1986.

[2] R. Carter and P. Fong, *The Sylow* 2*-subgroups of the finite classical groups*, J. Algebra **1** (1964), 139–151.

[3] C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. (2) **7** (1955), 14–66.

[4] R. Ree, *On some simple groups defined by C. Chevalley*, Trans. Amer. Math. Soc. **84** (1957), 392–400.

[5] A. J. Weir, *Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p*, Proc. Amer. Math. Soc. **6** (1955), 529–533.